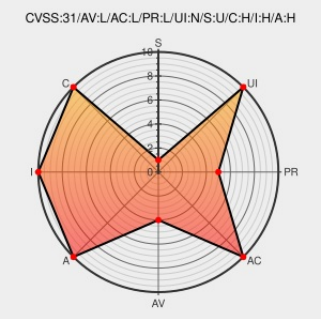
CVE-2021-32458

Published on: 05/27/2021 12:00:00 AM UTC

Last Modified on: 06/07/2021 07:08:00 PM UTC

CVE-2021-32458

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Home Network Security from Trendmicro contain the following vulnerability:

Trend Micro Home Network Security version 6.6.604 and earlier is vulnerable to an iotcl stack-based buffer overflow vulnerability which could allow an attacker to issue a specially crafted iotcl which could lead to code execution on affected devices. An attacker must first obtain the ability to execute low-privileged code on the target device in order to exploit this vulnerability.

CVE-2021-32458 has been assigned by security@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Trend Micro** - **Trend Micro Home Network Security** version **6.6.604 and below**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

TALOS-2021-1231 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2021-1231
TALOS-2021-1231 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	www.talosintelligence.com text/html	MISC www.talosintelligence.com/vulnerability_reports/TALOS-2021-1231
Security Bulletin: Trend Micro Home Network Security Multiple Vulnerabilities · Trend Micro for Home	helpcenter.trendmicro.com text/html	MISC helpcenter.trendmicro.com/en-us/article/TMKA-10337

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Home Network Security	All	All	All	en
Application	Trendmicro	Home Network Security	All	All	All	ja
Application	Trendmicro	Home Network Security	All	All	All	zh

cpe:2.3:a:trendmicro:home_network_security:*:*:*:en:*:*:*:*:

cpe:2.3:a:trendmicro:home_network_security:*:*:*:ja:*:*:*:*:

cpe:2.3:a:trendmicro:home_network_security:*:*:*:zh:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@SystemTek_UK	Trend Micro Home Network Security privilege escalation vulnerability [CVE-2021-32458] systemtek.co.uk/2021/05/trend-…	2021-05-24 19:55:18
@6townstechteam	Trend Micro Home Network Security privilege escalation vulnerability [CVE-2021-32458] systemtek.co.uk/2021/05/trend-…	2021-05-24 19:55:19
@twelvesec	#TrendMicro addresses 3 #vulnerabilities (CVE-2021-32457, CVE-2021-32458, CVE-2021-32459) in Home Network Security… twitter.com/i/web/status/1…	2021-05-26 14:34:03
@CVEreport	CVE-2021-32458 : A privilege escalation vulnerability exists in the tdts.ko chrdev_ioctl_handle functionality of Tr… twitter.com/i/web/status/1…	2021-05-27 11:06:45
/r/netcve	CVE-2021-32458	2021-05-27 11:41:29

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report